National Infrastructure Protection Center
CyberNotes

Issue #2001-20 *October 8, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between September 13 and October 4, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
3Com[1]	Multiple	Home Connect Cable Modem External with USB	A remote Denial of Service vulnerability exists in the firmware running the cable modem when connecting to the HTTP service and requesting a long string.	No workaround or patch available at time of publishing.	HomeConnect Cable Modem External with USB Denial of Service	Low	Bug discussed in newsgroups and websites. This can be exploited with a web browser.

[1] Securiteam, September 30, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
America Online[2]	Windows	AOL Instant Messenger/ Win32 4.7.2480, Win32 4.3.2229	A remote Denial of Service vulnerability exists due to the way HTML tags are handled.	No workaround or patch available at time of publishing.	AIM Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the press and other public media.
AmTote Interna-tional, Inc.[3]	Windows NT 4.0	Homebet	Two security vulnerabilities exist in the default installation because all account and corresponding PIN numbers are stored in the 'homebet.log' file which is world readable. This could let a malicious user obtain sensitive information.	Unofficial workaround: Change ACL on homebet.log to no access for IUSER accounts.	Homebet World Accessible Log and Brute Force	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Baltimore Technol-ogies[4]	Windows NT 4.0/2000	MAIL sweeper for SMTP 4.2, 4.2.1, 4.2.5	Two vulnerabilities exist due to the fact that malicious e-mail is not filtered at the gateway level, which could let a malicious user bypass restrictions and execute arbitrary code.	Upgrade to 4.2.6 available at: http://www.mimesweeper.baltimore.com/products/mailsweepersmtp/default.asp	MAILsweeper Script Filtering Bypass	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Charles Clark[5]	Windows 95/98/ME	Meteor FTP 1.0	A directory traversal vulnerability exists when a 'ls' command is submitted, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://207.202.218.172/meteorftp.exe	Meteor FTP Directory Traversal	Medium	Bug discussed in newsgroups and websites.
Cisco Systems[6]	Multiple	PIX Firewall 4.0-5.3	A Denial of Service vulnerability exists in the AAA authentication feature.	Upgrade available at: http://www.cisco.com/public/support/tac/home.shtml	PIX TACACS+ Denial of Service	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites. Exploit has been published.
Cisco Systems[7]	Multiple	PIX Firewall 4.4(7.202), 4.4(4), 5.1(4.206), 5.2(3.210), 6.0(1)	A vulnerability exists in the 'mailguard' feature, which could let a remote malicious user bypass SMTP command filtering.	Upgrade available at: http://www.cisco.com	PIX Firewall SMTP Content Filtering Evasion	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[2] Bugtraq, October 3, 2001.
[3] Securiteam, September 30, 2001.
[4] edvice Security Services, September 22, 2001.
[5] Cartel Informatique - Security Advisory, CARTSA-2001-03, September 28, 2001.
[6] Cisco Security Advisory, October 3, 2001.
[7] Cisco Security Advisory, Revision 1.0, September 26, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
COM2001[8]	Windows NT 4.0/2000	Alexis Server 2.0, 2.1	A vulnerability exists because a Java applet sends a user's voicemail password in cleartext over the Internet, which could let a remote malicious user gain unauthorized access to voicemail and PBX services.	Unofficial workaround (Bugtraq): Use a firewall to block access to port 8888 of the affected host. This will affect some functionality, such as call screening, etc.	Alexis Server Web Access Plaintext Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Compaq[9]	Unix	TruCluster 1.5	A Denial of Service vulnerability exists when a system is portscanned without a DNS PTR record in DNS. This can result in corrupted or destroyed data, Denial of Service, and even hardware damage.	No workaround or patch available at time of publishing.	TruCluster Port Scan Denial of Service	Low/ Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Compaq[10]	Unix, OpenVMS	All Compaq Web-enabled Management Software	A buffer overflow vulnerability exists in a component of the software, which could let a remote malicious user execute arbitrary code.	Patch available at: ftp://ftp.compaq.com/pub/softpaq/sp17501-18000/	Compaq Management Agents Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Francisco Burzi[11]	Multiple	PHP Nuke 5.2 and prior	A vulnerability exists in the administrative component of 'admin.php', which could let a remote malicious user overwrite arbitrary webserver writeable files with data from arbitrary webserver readable files.	No workaround or patch available at time of publishing.	PHPNuke Remote File Copy	**High**	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
Hans Wolters[12]	Unix	phpReview 0.9.0 rc2, 0.9-final, 0.2.1, 0.2.0, 0.1.0	A cross-site scripting vulnerability exists because HTML user-submitted tags are not filtered, which could let a malicious user execute arbitrary script.	Upgrade available at: http://phpreview.nl.linux.org/	phpReview Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Hewlett Packard[13]	Multiple	HP9000 Series 700/800 running HP-UX releases 11.11, 11.00, 11.04, 10.20, 10.10, 10.01	A Denial of Service vulnerability exists in the 'cu(1)' command, typically used for host to host communications.	Patch available at: PHCO_23909, PHCO_22766, PHCO_23424, PHCO_22764, PHCO_22765, PHCO_22763 ftp.itrc.hp.com:~ftp/export/patches/hp-ux_patch_matrix	HP 'cu(1)' Command Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett Packard[14]	Unix	HP-UX 11.0, 11.11	A Denial of Service vulnerability exists in the 'rpcbind' implementation because malformed RPC requests crash portmapper.	Patch available at: PHNE_24034 PHNE_24035 http://itrc.hp.com	HP-UX RPCBind Random Buffer Overflow Denial of Service	Low	Bug discussed in newsgroups and websites.

[8] Bugtraq, September 27, 2001.
[9] Bugtraq, September 25, 2001.
[10] Compaq Management Software Security Advisory, SSRT0758, September 28, 2001.
[11] Twlc Security Advisory, September 24, 2001.
[12] SecurityFocus, October 1, 2001.
[13] Hewlett-Packard Company Security Bulletin, HPSBUX0109-167, September 24, 2001.
[14] Hewlett-Packard Company Security Bulletin, HPSBUX0110-169, October 2, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard[15]	Windows NT 4.0/2000, Unix	OpenView Network Node Manager 5.01, 6.1, 6.2	A vulnerability exists in the Network Node Manager (NNM), which could let a malicious user execute arbitrary code.	Update available at: http://ovweb.external.hp.com/cpe/patches/	OpenView Network Node Manager Arbitrary Privilege Elevation	**High**	Bug discussed in newsgroups and websites.
Hylafax[16]	Unix	Hylafax 4.1	A format string vulnerability exists because input isn't sufficiently sanitized when the hostname is entered, which could let a malicious user gain elevated privileges and execute arbitrary code.	No workaround or patch available at time of publishing.	Hylafax Hostname Format String	**High**	Bug discussed in newsgroups and websites.
IBM[17]	Unix	HACMP 4.4	A remote Denial of Service vulnerability exists due to the way portscans are handled by High Availability Cluster Multiprocessing (HACMP) control application	No workaround or patch available at time of publishing.	HACMP Port Scan Denial of Service	Low	Bug discussed in newsgroups and websites. A portscanning utility is required to take advantage of this vulnerability.
Michael Barretto[18]	Multiple	CardBoard 2.0	A vulnerability exists due to the improper filtering of certain types of user-supplied input, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	CardBoard Remote Command Execution	**High**	Bug discussed in newsgroups and websites.
Microsoft[19]	Mac OS X 10.1	Microsoft Internet Explorer bundled with Mac OS X 10.1	A vulnerability exists when IE downloads a .bin, or .hqx file it will automatically decompress the file and execute the application, which could let a malicious user execute arbitrary code.	Unofficial workaround: Under IE's preferences and download options, uncheck automatically decode .BIN and .HQX files. Although it will still decompress these files, it won't automatically execute them.	Mac OS X .bin and .hqx Decompress File	**High**	Bug discussed in newsgroups and websites.
Microsoft[20]	Windows 2000	Exchange Server 2000, Exchange Server 2000SP1	A remote Denial of Service vulnerability exists in Outlook Web Access (OWA) because it will accept and process a request for an item in an authenticated user's mailbox without verifying first that the folder structure is valid.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-049.asp	Microsoft Exchange OWA Server Resource Starvation CVE Name: CAN-2001-0666	Low	Bug discussed in newsgroups and websites. This can be exploited with a web browser.

[15] Hewlett-Packard Company Security Bulletin, HPSBUX0110-170, October 2, 2001.
[16] Bugtraq, September 24, 2001.
[17] Bugtraq, September 24, 2001.
[18] Securiteam List Digest, October 1, 2001.
[19] MacSlash, October 2, 2001.
[20] Microsoft Security Bulletin, MS01-049, September 26, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[21]	Windows 95/98/ME/ NT 4.0/2000	Excel 98, 2001 Macintosh Edition, Excel 97, 2000, 2002; PowerPoint 97, 2000, 2002, PowerPoint 98, 2001 Macintosh Edition	A vulnerability exists in the way macros are detected which could let a malicious user bypass macro checking and execute arbitrary macro code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-050.asp	Microsoft Excel and PowerPoint Macro Security Bypass CVE Name: CAN-2001-0718	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Multiple Vendors[22]	Unix	Compaq Tru64 4.0g, 5.0f, 5.0a, 5.1a, 5.1; HP HP-UX 10.1-11.11, HP HP-UX (VVOS) 10.24, 11.0.4; IBM AIX 4.3-4.3.3, 5.1; SGI IRIX 5.2- 6.4; Sun Solaris 1.1-8.0	A format string vulnerability exists in the ToolTalk database, which could let a remote malicious user cause a Denial of Service or gain root access.	Contact your vendor for patch.	Multiple CDE Vendor ToolTalk Database Server Format String	Low/**High**	Bug discussed in newsgroups and websites.

[21] Microsoft Security Bulletin, MS01-050, October 4, 2001.
[22] Internet Security Systems Security Advisory, October 2, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[23]	Multiple	CCCSoft-ware CCC 0.90-1.03; topher1 kenobe AWOL 1.0-2.1; Derek Leung pSlash 0.70; Sebastian Bunka myphpPage tool 0.4.3-1; Peace Works Computer Consulting Phormation 0.9.1; Tobias Ratschiller phpAdsNew 2.0beta 5; Bharat Mediratta Gallery 1.2.1; Haakon Nilsen SIPS 0.3; Paul M. Jones Phorecast 0.30a; Zorbat Zorbstats 0.8; Grant Horwood Webodex 1.0; Actionpoll 1.1.1; Marc Logemann More.group ware 0.5.1; Emergencies Personnel Information System Empris 20010908, 20010810, 0.4; Dark Hart Portal DarkPortal-unix 0.1.16-0.1.18	A vulnerability exists in the '$include' variable, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple Vendors Remote Arbitrary Code Execution	High	Bug discussed in newsgroups and websites. This can be exploited with a web browser.

[23] Bugtraq, October 2, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MySQL AB[24]	Unix	MySQL 3.23.x, WinMySQL admin 1.1	A vulnerability exists in the 'my.ini' file because the contents are stored in plain text, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WinMySQL admin Plain Text Password Storage	Medium	Bug discussed in newsgroups and websites.
National Science Foundation [25]	Unix	Squid Web Proxy 2.4, 2.4DEVEL2, 2.4DEVEL4, 2.4PRE-STABLE, 2.4PRE-STABLE2, 2.4STABLE 1, 2.3, 2.3STABLE 2-2.3STABLE5	A Denial of Service vulnerability exists when a specially crafted "mkdir-only" PUT request is sent.	Patch available at: http://www.squid-cache.org/bugs/showattachment.cgi?attach_id=38	Squid Web Proxy Cache Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Networks Associates Incor-porated[26]	Windows NT 4.0/2000, Unix	PGP Keyserver 7.0, 7.0.1	A vulnerability exists in the PGP key server due to a misconfiguration in the default permissions, which could let a remote malicious user gain administrative access to the interface.	Workaround available at: http://www.pgp.com/support/product-advisories/keyserver.asp	PGP Keyserver Web Administration Interface Authentication Bypassing	**High**	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
OpenSSH[27]	Unix	OpenSSH 2.5-2.5.2, 2.9	A vulnerability exists when two keys of different types appear successively in the '.authorized_keys2' file, which could let a remote malicious user bypass some access control and log in from unauthorized hosts.	Upgrade available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/openssh-2.9.9.tgz	OpenSSH Key Based Source IP Access Control Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Positive Software[28]	Windows 2000, Unix	H-Sphere 1.5, 2.0, 2.05, 2.06	A vulnerability exists in the 'template_name' variable, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	H-Sphere Arbitrary File Disclosure	Medium	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
QPC Software[29]	Windows 95/98/ME/ NT 4.0/2000	QVT/Term 5.0	A remote Denial of Service vulnerability exists in the FTP daemon when an unusually long string of arbitrary characters is submitted.	No workaround or patch available at time of publishing.	QVT/Term FTP Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[24] Bugtraq, October 2, 2001.
[25] Securiteam, September 24, 2001.
[26] SNS Advisory No.43, September 28, 2001.
[27] OpenSSH Security Advisory, September 26, 2001.
[28] Bugtraq, September 25, 2001.
[29] Bugtraq, September 25, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RedHat[30]	Unix	Linux 7.1	A race condition vulnerability exists in 'initscript' that is distributed with the setserial package, which could let a malicious user overwrite system files, causing a Denial of Service, and potentially gain elevated privileges.	**RedHat workaround:** 1. Use a Red Hat supplied kernel. 2. If the kernel must be recompiled, make serial support part of the kernel (versus modular). 3. Under no circumstance should the init script supplied with setserial be used. The following command is recommended by Red Hat to disable the setserial init script: */sbin/chkconfig serial off*	RedHat Setserial Init Script Predictable Temporary File	Medium	Bug discussed in newsgroups and websites.
Sendmail Consortium [31]	Unix	Sendmail 8.9.3-8.11.5, 8.12beta5, 8.12beta7, 8.12beta10, 8.12beta12, 8.12beta16, 8.12	Several vulnerabilities exist: a Denial of Service vulnerability exists because the key configuration variables can be changed by a malicious user; and a vulnerability exists in the 'sendmail' utility, which could let a malicious user gain elevated privileges.	Upgrade available at: ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.12.1.tar.Z	Sendmail Multiple Vulnerabilities CVE Names: CAN-2001-0713, CAN-2001-0714, CAN-2001-0715	Low/ Medium	Bug discussed in newsgroups and websites.
SLRN Develop-ment Team[32]	Unix	slrn 0.9.6.2	A vulnerability exists in the shell script handling code, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://security.debian.org/dists/stable/updates/main/	SLRN Arbitrary Shell Script Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro-systems, Inc.[33]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists in the 'rpc.yppasswdd' implementation, which could let a local and remote malicious user execute arbitrary code with full system privileges.	Patch available at: http://sunsolve.Sun.COM/pub-cgi/	Solaris rpc.yppasswdd Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Valve Software[34]	Windows 95/98/NT 4.0	Half-Life 1.1.0.8	A buffer overflow vulnerability exists in the /Connect command, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Half-Life Client Side Connect Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

[30] Red Hat Security Advisory, RHSA-2001:110-05, September 19, 2001.
[31] RAZOR Advisory, October 1, 2001.
[32] Debian Security Advisory, DSA-078-1, September 24, 2001.
[33] Sun Alert Notification, September 13, 2001.
[34] Bugtraq, September 20, 2001.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between September 13 and October 3, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 9 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
October 3, 2001	**Aimrape.tar.gz**	**A remote denial of service exploit for AOL Instant Messenger (AIM) vulnerability.**
October 3, 2001	Hackingguide3.1.pdf	A guide for breaking into computer networks from the Internet that includes host enumeration, scanners, custom tools, protocols, windows information, and much more.
September 30, 2001	**Homebetlog.pl**	**Perl script which exploits the AmTote Homebet World Accessible Log and Brute Force vulnerabilities.**
September 28, 2001	Alpha-fmtstr.txt	How to Guide, "How to Exploit Format String Vulnerabilities under Alpha Linux" that includes techniques and example code.
September 28, 2001	Maj1944-xpl.pl	Perl exploit script for the Majordomo v1.94.4 vulnerability.
September 26, 2001	Gtkskan-0.2.tgz	A GTK tool that scans for 802.11b networks using WAVELAN/Aironet hardware and Linux wireless extensions. It includes the ability to log coordinates of found networks from a NMEA-compatible GPS device, and it can be linked to a serial port.
September 26, 2001	Thcrut-0.1.tar.gz	A local network discovery tool developed to brute force its way into WVLAN access points, which offers: ARP-request on IP-ranges and identifies the vendor of the NIC, spoofed DHCP, BOOTP, and RARP requests, ICMP-address mask request and router discovery techniques.
September 26, 2001	Wardrive-2.0.tar.gz	A Linux-based tool for mapping your city for WAVELAN networks with a GPS device while you are driving a car or walking through the streets; it supports NMEA GPS devices.
September 13, 2001	Ypexp.tar.gz	Script which exploits the Solaris rpc.yppasswdd Buffer Overflow vulnerability.

Trends

Probes/Scans:

- **CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.**

Other:

- **The National Infrastructure Protection Center (NIPC) continues to observe hacking activity targeting the e-commerce or e-finance/banking industry. For more information, see NIPC ADVISORY 01-023 located at: http://www.nipc.gov/warnings/advisories/2001/01-023.htm. The most prevalent exploit being used to gain access to targeted systems is the Unicode vulnerability found in the Microsoft Internet Information Services (IIS) web server software, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-086.asp**
- An e-mail message claiming to come from the SecurityFocus ARIS Analyst Team and TrendMicro includes an attachment that claims to be a fix for the Nimda worm. Instead, the attachment is a Trojan program called Shake.Trojan (see Trojan Section) which is designed to do damage to the systems of anyone who runs the software.
- **The National Infrastructure Protection Center expects to see an upswing in incidents as a result of the tragic events of September 11, 2001. For more information, see NIPC ADVISORY 01-020, available at http://www.nipc.gov/warnings/advisories/2001/01-020.htm.**
- **The National Infrastructure Protection Center has received numerous reports that a new worm, named W32.Nimda.A@MM, is propagating extensively through the Internet worldwide. The worm is exhibiting many traits of recently successful malicious code attacks such as CODE RED but it is not simply another version of that worm. For more information, see NIPC ADVISORY 01-022, available at: http://www.nipc.gov/warnings/advisories/2001/01-022.htm.**
- **The National Infrastructure Protection Center expects an increase in Distributed Denial of Service (DDoS) attacks. For more information, see NIPC ADVISORY 01-021 located at: http://www.nipc.gov/warnings/advisories/2001/01-021.htm.**
- **Recently, the cyber security community received numerous reports of intruders using the buffer overflow vulnerability in the Telnet daemon program. For more information, see NIPC ASSESSMENT 01-019, available at: http://www.nipc.gov/warnings/assessments/2001/01-019.htm. This vulnerability has the potential to impact the victim by allowing an intruder to copy, delete, or execute any program on the victim's system. A new worm called "x.c," designed to exploit this vulnerability, has also been discovered.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

PE_DION.A (Aliases: DION.A, Win32.Dion, W95.Dion) (File Infector Virus): This is a non-destructive, memory-resident, and polymorphic PE virus. Upon execution, it copies itself to an 8-digit random filename with a .DLL extension in the Windows System directory and stays in memory. Next, this virus infects running applications as they are closed. It inserts its encrypted chunks of code into the body of the host file so that it increases the size of the infected file by 5,036 bytes. It also modifies the first few bytes of the entry point of an infected file, but it only moves the body of the infected file to the end of its inserted viral code. Occasionally, infected files do not execute due to bugs in the virus code, which changes with every infection.

VBS.Erul.A@mm (Alias: VBS.Alert.A@mm) (Visual Basic Script Worm): This is a Visual Basic Script (VBS) worm that sends e-mail to all contacts that are in the Microsoft Outlook address book. It searches for all files that have the extension .vbs and overwrites them with itself. The virus also creates a copy of itself in the C:\Windows folder as Failure.dll.vbs.

W32.HLLW.Giwin (Win32 Virus): This is a simple worm that copies itself to the root of drive C, C:\Windows, and C:\Windows\System as Setup32.exe. It also creates 50 copies of itself in each of these locations as _##_.exe, where ## is a number between 1 and 50. This worm also copies itself to the floppy disk if one is present in the floppy disk drive.

W97M/Camino.a@MM (Alias: W97M.Volcano.A@mm) (Word 97 Macro Virus): This virus infects Microsoft Word 97 (or higher) documents and templates. The virus consists of one module named Volcano containing the following macros:

- FileOpen()
- AutoClose()
- Infectar()
- Enviar()
- r()
- ToolsMacro()
- FileTemplates()
- ViewVBCode()

Upon opening a document, the virus checks to see if Word 2000 is running, and if so, it disables Tools/Macro/Security menu and sets the Security level to low. This is done by changing the value of Level in the registry key:

HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security

If the version of Word is not 2000, then the virus disables the Tools|Macro menu and disables the following options: ConfirmConversions, VirusProtection, SaveNormalPrompt, CheckGrammarAsYouType, CheckGrammerWithSpelling and SavePropertiesPrompt. The virus also disables the settings: ScreenUpdating, DisplayAlerts, and the Escape key. It goes on to check if the registry key:

HKEY_CURRENT_USER\Software\Microsoft\Office\Volcano?=...Rol12

is present, and uses Microsoft Outlook to send an e-mail to the first 50 addresses in the Address Book, attaching the infected file. The virus then sets the registry key value:

HKEY_CURRENT_USER\Software\Microsoft\Office\Volcano?=...Rol12

It searches to see if the following folders exist: C:\WINNT\SYSTEM\or C:\WINDOWS\SYSTEM\. Then it checks to see if a registry key, exists and if not it creates it:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Run\Vc12=C:\WINNT\SYSTEM\Vc12.Vbs

or (depending on the operating system)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Run\Vc12=C:\WINDOWS\SYSTEM\Vc12.Vbs

The virus then exports its code to the file C:\WINDOWS\SYSTEM\Vc12.dll and creates the file C:\WINDOWS\SYSTEM\Vc12.Vbs. This file will be run when Windows is started, causing the Normal Template to be infected with the virus. It infects the system by checking the Normal Template to see if the module "Volcano" is present. If not, the virus exports its code to "C:\Volcano.dll." This action is performed on each open document as well.

W97M.Likon.A (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and the global template Normal.dot. The virus is activated on Autoexec, AutoOpen, and DocumentChange. When executed, it does the following: First the virus checks whether the date is April 17, 2000 or later. If it is before this date or if a file named C:\Nokill.pls exists, it does nothing. Otherwise, it creates two files, C:\Start, which contains a response for the Format command, and C:\Autoexec, which contains the Format a: command. Since the file does not have the .bat extension, it will never be executed. The virus next checks for a previous infection by searching for the presence of the CloseA module. If it is not present in any open documents or templates, it exports temporary files for each module. The exports are named C:\Test-0-2.bas and C:\Test-0-3.bas. These files are deleted after the modules are reimported.

W97M.Tador.A (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and the global template Normal.dot. It also attempts to connect to a specific FTP site; if it is successful, it performs the following actions:

- It downloads and then runs an executable file.
- It uploads your user name and the number of infections on your system.

X97M.Ellar.A (Excel 97 Macro Virus): This is a Microsoft Excel virus that spreads by saving an infected workbook in the Microsoft Excel startup folder. It also deletes all Excel files that are in the same folder as the virus. When it is activated, this virus performs the following actions:

- It changes the Save, Save As, and Macro menu commands and the Ctrl+S key combination to its own Save (which also infects).
- It deletes all .xls files in the same folder as the virus, except for files that are currently open.
- It deletes all sheets in the workbook, except for the one named "0."
- It makes the workbook hidden.
- It saves the infected workbook in the Excel startup folder as Microsoft.xls

Because the workbook is hidden, the user will not notice that it is loaded the next time that you start Excel.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
Adshow	N/A	CyberNotes-2001-17
AOL.PWSteal.86016	N/A	CyberNotes-2001-14
Artic	0.6 beta	CyberNotes-2001-14
Asylum	N/A	CyberNotes-2001-18
Backdoor.Bionet.318	N/A	CyberNotes-2001-13
Backdoor.Bionet.40a	N/A	CyberNotes-2001-14
Backdoor.Darkirc	N/A	CyberNotes-2001-15
Backdoor.G_Door	N/A	CyberNotes-2001-18
Backdoor.IRC.Critical	N/A	CyberNotes-2001-19
Backdoor.IRC.Flood	N/A	CyberNotes-2001-16
Backdoor.MiniCommander:	N/A	CyberNotes-2001-16
Backdoor.Penrox	N/A	CyberNotes-2001-17
Backdoor.SMBRelay	N/A	CyberNotes-2001-10
Backdoor.Teste	N/A	CyberNotes-2001-16
Backdoor.Way	N/A	CyberNotes-2001-18
Backdoor.WLF	N/A	CyberNotes-2001-08
Backdoor-QN	N/A	CyberNotes-2001-13
Backdoor-QO	N/A	CyberNotes-2001-13
Backdoor-QR	N/A	CyberNotes-2001-13
Backdoor-QT	N/A	CyberNotes-2001-14
Backdoor-QV	N/A	CyberNotes-2001-14
Backdoor-QZ	N/A	CyberNotes-2001-14
BAT.Black	N/A	CyberNotes-2001-11
Bat.FAGE.1482	N/A	CyberNotes-2001-15
Bat.Hexvirus.1414	N/A	CyberNotes-2001-15
Bat.PG94.3964	N/A	CyberNotes-2001-15

Trojan	Version	CyberNotes Issue #
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_FORMATC.K	N/A	CyberNotes-2001-13
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07
CodeRed II	II	CyberNotes-2001-16
DMsetup.IRC.Worm	N/A	CyberNotes-2001-13
DonaldD.Trojan.C	N/A	CyberNotes-2001-19
EIC.Trojan	N/A	CyberNotes-2001-14
Eurosol	N/A	CyberNotes-2001-10
Fatal Connections	2.0	CyberNotes-2001-09
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
Goga	N/A	CyberNotes-2001-12
Gribble	N/A	CyberNotes-2001-19
HackTack	N/A	CyberNotes-2001-18
IRC/FinalBot	N/A	CyberNotes-2001-18
Jammer Killah	1.2	CyberNotes-2001-10
JAVA_STORM.A	N/A	CyberNotes-2001-13
JS.Alert.Trojan	N/A	CyberNotes-2001-19
JS.Seeker.B	N/A	CyberNotes-2001-18
JS.StartPage	N/A	CyberNotes-2001-07
JS_OFFENSIVE.A	N/A	CyberNotes-2001-17
JS_ZOPA.A	N/A	CyberNotes-2001-14
KillMBR.g	N/A	CyberNotes-2001-16
Lil Witch FTP	1.0	CyberNotes-2001-19
Noob	4.0	CyberNotes-2001-09
PERL/WSFT-Exploit	N/A	CyberNotes-2001-11
Phoenix	2.1.28	CyberNotes-2001-18
PWS.Cain.dr	N/A	CyberNotes-2001-19
PWSteal.Trojan.D	N/A	CyberNotes-2001-13
QDel172	N/A	CyberNotes-2001-17
Remote Shell Trojan	N/A	CyberNotes-2001-19
SadCase.Trojan	N/A	CyberNotes-2001-09
Scarab	1.2c	CyberNotes-2001-10
SennaSpy Generator	N/A	CyberNotes-2001-13
Shake.Trojan	**N/A**	**Current Issue**
StealVXS	N/A	CyberNotes-2001-17
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog-C	N/A	CyberNotes-2001-08
Troj/PsychwardB	N/A	CyberNotes-2001-14
Troj/Slack	N/A	CyberNotes-2001-14
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_ALLGRO.A	N/A	CyberNotes-2001-17
TROJ_APOST.A	N/A	CyberNotes-2001-18
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_BADTRANS.A	N/A	CyberNotes-2001-08
TROJ_BADY	N/A	CyberNotes-2001-15
TROJ_BCKDOR.G2.A	N/A	CyberNotes-2001-11
TROJ_CAFEIN111.A	N/A	CyberNotes-2001-14
TROJ_CHOKE.A	N/A	CyberNotes-2001-13
TROJ_DSNX.A	N/A	CyberNotes-2001-17
TROJ_EUTH.152	N/A	CyberNotes-2001-08
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_HAI.A	N/A	CyberNotes-2001-17
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09

Trojan	Version	CyberNotes Issue #
TROJ_ICMPBOMB.A	N/A	CyberNotes-2001-17
TROJ_IDENTD.B	N/A	CyberNotes-2001-11
TROJ_IE_XPLOIT.A	N/A	CyberNotes-2001-08
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09
TROJ_INVALID.A	N/A	CyberNotes-2001-18
TROJ_IRC_NETOL.A	N/A	CyberNotes-2001-14
TROJ_JESTRO.A	**N/A**	**Current Issue**
TROJ_JOINER.I	N/A	CyberNotes-2001-08
TROJ_KEYLOG.25	N/A	CyberNotes-2001-17
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_LATINUS.SVR	N/A	CyberNotes-2001-12
TROJ_LEAVE.A	N/A	CyberNotes-2001-13
TROJ_LINONG.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.B	N/A	CyberNotes-2001-13
TROJ_MATCHER.A	N/A	CyberNotes-2001-08
TROJ_MEGA.A	N/A	CyberNotes-2001-12
TROJ_MODNAR.A	N/A	CyberNotes-2001-17
TROJ_MOONPIE.A	N/A	CyberNotes-2001-11
TROJ_MSWORLD.A	N/A	CyberNotes-2001-12
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09
TROJ_MUSTARD.A	N/A	CyberNotes-2001-19
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NEWPIC.A	N/A	CyberNotes-2001-17
TROJ_NEWSAGENT.A	N/A	CyberNotes-2001-16
TROJ_NEWSFLOOD.A	N/A	CyberNotes-2001-13
TROJ_OPTIX.SVR	N/A	CyberNotes-2001-17
TROJ_PICSHOW.A	N/A	CyberNotes-2001-10
TROJ_PSW.GINA.A	N/A	CyberNotes-2001-13
TROJ_SCOUT.A	N/A	CyberNotes-2001-08
TROJ_SIRCAM.A	N/A	CyberNotes-2001-15
TROJ_SPYBOY.A	N/A	CyberNotes-2001-18
TROJ_VAMP.A	N/A	CyberNotes-2001-13
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_VOTE.A	A	CyberNotes-2001-19
TROJ_VOTE.B	**B**	**Current Issue**
TROJ_VOTE.C	**C**	**Current Issue**
TROJ_WARHOME.A	N/A	CyberNotes-2001-12
TROJ_WHISTLER.A	N/A	CyberNotes-2001-19
TROJ_WINMITE.10	N/A	CyberNotes-2001-08
TROJ_ZERAF.A	N/A	CyberNotes-2001-18
Trojan.Assault.10	10	CyberNotes-2001-15
Trojan.Bat.Live4:	N/A	CyberNotes-2001-16
Trojan.Billrus.Texto	N/A	CyberNotes-2001-14
Trojan.Diagcfg	N/A	CyberNotes-2001-15
Trojan.JS.Clid.gen	N/A	CyberNotes-2001-17
Trojan.JS.Cover	N/A	CyberNotes-2001-18
Trojan.Lornuke	N/A	CyberNotes-2001-14
Trojan.Offensive	N/A	CyberNotes-2001-17
Trojan.Pounds	N/A	CyberNotes-2001-18
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.VBS.PWStroy	N/A	CyberNotes-2001-14
Trojan.VirtualRoot	N/A	CyberNotes-2001-16
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan.Xtratank	N/A	CyberNotes-2001-17

Trojan	Version	CyberNotes Issue #
Trojan.Zeraf	N/A	CyberNotes-2001-17
Trojan.ZeroBoot	N/A	CyberNotes-2001-19
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.AutoExec.Trojan	N/A	CyberNotes-2001-16
VBS.Blank.A	N/A	CyberNotes-2001-14
VBS.Fiber.C	N/A	CyberNotes-2001-18
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Natas	N/A	CyberNotes-2001-16
VBS.Over.Trojan	N/A	CyberNotes-2001-10
VBS.Phybre	N/A	CyberNotes-2001-12
VBS.Reset	N/A	CyberNotes-2001-12
VBS.SystemColor.A	N/A	CyberNotes-2001-11
VBS.Trojan.Icon	N/A	CyberNotes-2001-18
VBS.Trojan.Lariara	N/A	CyberNotes-2001-18
VBS.Zeichen.A	N/A	CyberNotes-2001-08
VBS.Zync.A	N/A	CyberNotes-2001-17
VBS_HAPTIME.A	N/A	CyberNotes-2001-09
VBS_IESTART.A	N/A	CyberNotes-2001-11
W32.BrainProtect	N/A	CyberNotes-2001-07
W32.Leave.B.Worm	N/A	CyberNotes-2001-14
W32.Whiter.Trojan	**N/A**	**Current Issue**
Y3K Rat	1.6	CyberNotes-2001-11

Shake.Trojan (Alias: Win32.Shaker) : This Trojan is being distributed as a copy of the W32/Nimda@MM virus on a website which distributes viruses. It is a simple Trojan that contains one payload; to shake the top most window back and forth repeatedly and quickly. The Trojan does not configure itself to load at startup or copy itself to any other directory. A simple reboot unloads the program from memory. When run a message box is displayed, "shaking." Clicking the OK button does not unload the program. It must be unloaded by terminating the process, or rebooting Windows.

TROJ_JESTRO.A (Alias: JESTRO.A): This is a fake e-mail message claiming to come from SecurityFocus' ARIS system and Trend Micro is being used to send a backdoor program disguised as Trend Micro's NIMDA fix tool, called FIX_NIMDA.EXE. This backdoor program creates two Trojan files, TROJ_BIONET318.A and TROJ_HUKKEY.A. It is also responsible for logging all keystrokes from the keyboard and for saving these keystrokes in a KEYLOG.TXT file. It also shares an infected system's local drives C:\ through Z:\, which it hides with a dollar sign. These messages do not come from Security Focus or Trend Micro. Trend Micro does not send e-mails with executable attachments, unless specifically requested to do so by individual customers.

TROJ_VOTE.B (Aliases: Anti_TeRRoRisM.exe, VBS_VOTE.B): This destructive, mass-mailing worm is a variant of TROJ_VOTE.A. It propagates via Microsoft Outlook by sending e-mails to all addresses listed in an infected user's address book. It arrives in an e-mail with the following:

> Subject: This War Must Be Done !
> Message Body:
> Hi
> We Must Fight , We Must ReMemBer Our Victims!
> No Peace Before KiLLing TeRRoRists!
> Attachment: Anti_TeRRoRisM.exe

It also modifies the infected user's Internet Explorer start page and drops VBS files which parse drives and directories in search of HTM and HTML files and overwrites them with the following string:

> AmeRiCa ...Few Days WiLL Show You What We Can Do!!! It's Our Turn >>> ZaCkEr is So Sorry For You

This program requires that the Visual Basic Runtime Library, MSVBVM50.DLL, be installed in order to execute.

TROJ_VOTE.C (Alias: VOTE.C): This Trojan is a variant of TROJ_VOTE.A and TROJ_VOTE.B. It propagates via Microsoft Outlook by sending itself to all addresses listed in an infected user's address book. It arrives in an e-mail with the following:

Subject: Fwd:Peace BeTween AmeriCa And IsLam!
Message Body:
Hi!
iS iT A waR Against AmeriCa Or IsLam!
Let's Vote To Live in Peace!
Attachment: WTC.EXE

It creates a copy of itself in the Windows folder, and then creates and executes the following files:

- DaLaL.vbs
- Mixdalal.vbs
- WAIL.vbs

It searches for and overwrites all .HTML and .HTM files in an infected user's system with a text string, and also modifies the infected user's Internet Explorer startup page.

W32.Whiter.Trojan (Aliases: Trojan.Win32.Whiter.A, W95/Phistler.A): This Trojan horse arrives as a key generator for Windows XP (Whistler). When this Trojan is activated, it may present, in Notepad, what appears to be a valid key. This key, however, is not valid and is just a string of randomly generated numbers. At the same time, the Trojan inserts itself into the system so that the next time the victim starts the computer, it will delete all the files from the hard disk.